RSAC 2025 Conference

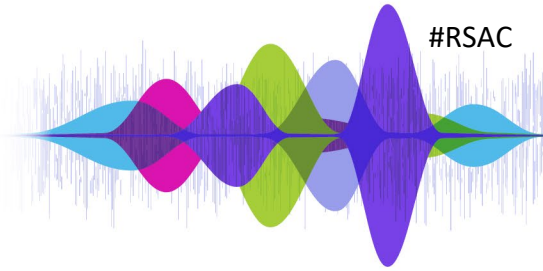
Many Voices.
One Community.

SESSION ID: APP-W01

Software Security Maturity Models SAMM vs. BSIMM: Which is Better?

Nariman AGA-TAGIYEV

Application Security Architect
Dassault Systemes SE
https://www.linkedin.com/in/aganariman/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Introduction and Acknowledgements

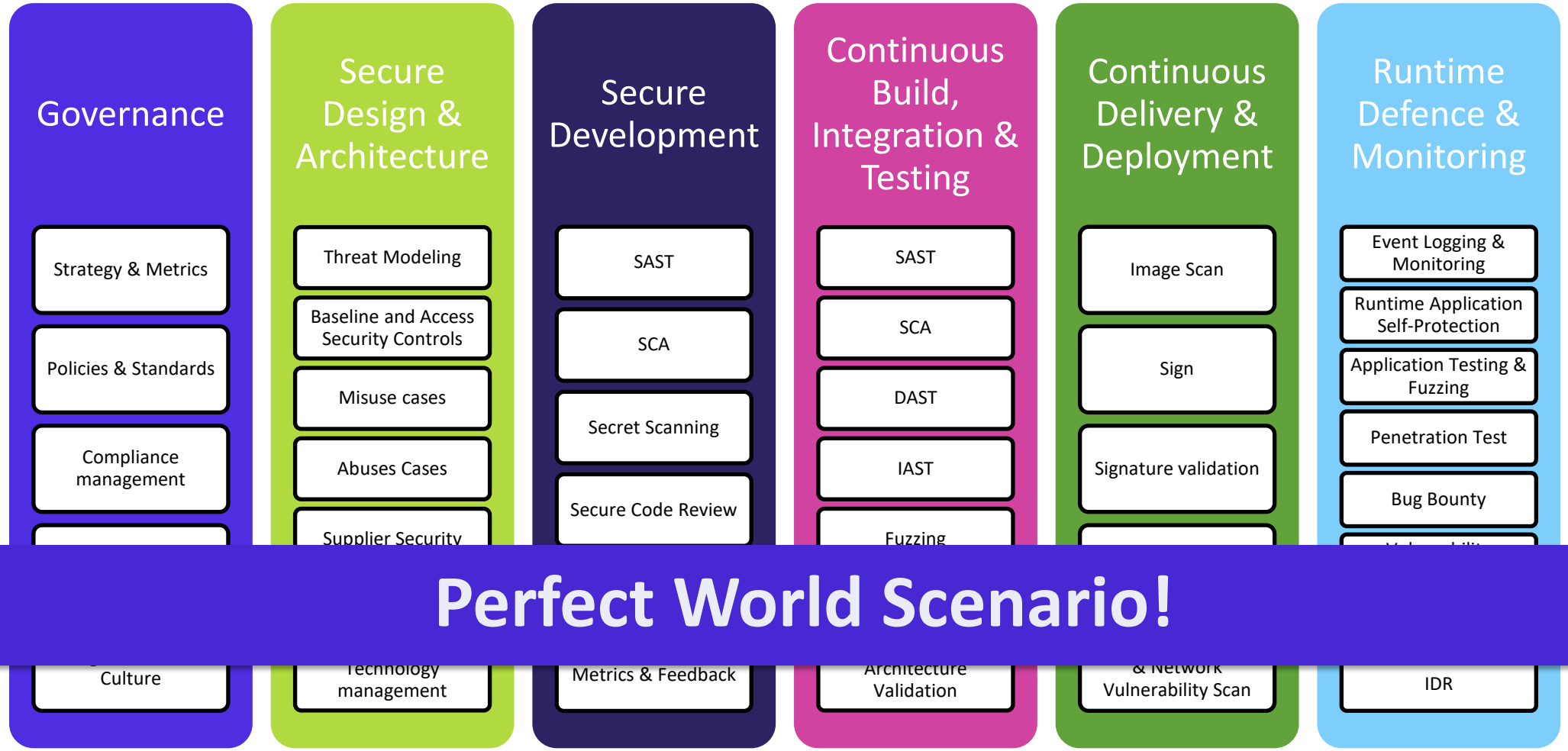
Caroline WONG

- Director of Cybersecurity @Teradata
- 20 years in Information Security
- Author of “Security Metrics: A Beginner’s Guide”
- LinkedIn Learning courses on cybersecurity
- Led > 30 BSIMM assessments, contributor for ISO27034

Nariman AGA-TAGIYEV

- Cybersecurity Architect @Dassault Systèmes
- Core team member @OWASP SAMM
- Secure coding and threat modeling trainer @SecureHabits
- 24 years in software development, 8 years in product security

Your Global SSDLC Policy



Perfect World Scenario!

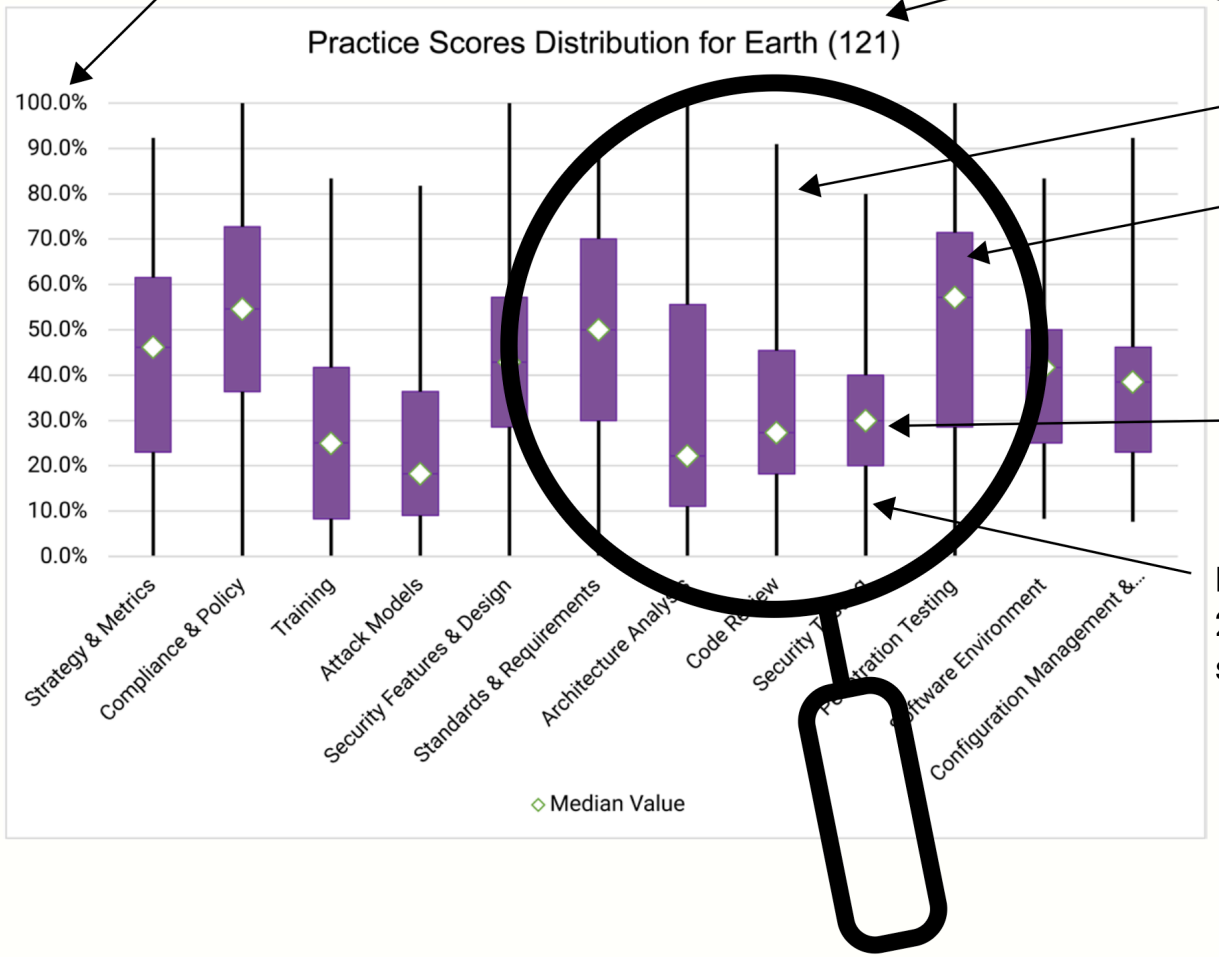
Maturity Models

Framework that helps organizations **assess** and **improve** their software security practices through defined levels of maturity.

BSIMM

Vertical axis is the percentage of activities in the practice vs. how many were observed from that practice. A firm scoring 5 activities from a practice with 10 activities total would score 50%

This chart is for the entire BSIMM data pool "Earth"



How the top 25% of firms scored

Box shows where the middle 50% of the firms scored

White diamond shows the median score

How the bottom 25% of firms scored

OWASP SAMM

Governance
Design
Implementation
Verification
Operations
Strategy & Metrics
Create & promote
Measure & improve
Threat Assessment
Application risk profile
Threat modeling
Secure Build
Build process
Software dependencies
Architecture Assessment
Architecture validation
Architecture compliance
Incident Management
Incident detection
Incident response
Policy & Compliance
Policy & standards
Compliance management
Security Requirements
Software requirements
Supplier security
Secure Deployment
Deployment process
Secret management
Requirements-driven Testing
Control verification
Misuse/abuse testing
Environment Management
Configuration hardening
Patch & update
Education & Guidance
Training & awareness
Organization & culture
Secure Architecture
Architecture design
Technology management
Defect Management
Defect tracking
Metrics & feedback
Security Testing
Scalable baseline
Deep understanding
Operational Management
Data protection
Legacy management
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B

Maturity Levels

Activity score:
YES | NO

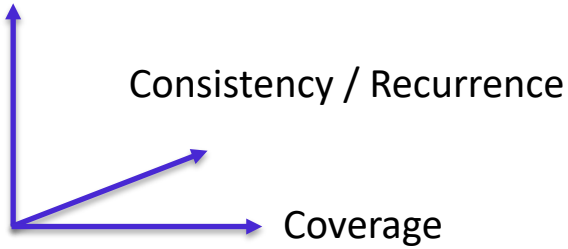
Questions and criteria are defined
for assessment leads
but are not available for public use

STRATEGY & METRICS		
Description	**BSIMM Community**	**Observed?**
LEVEL 1		
Publish Processes	80%	✓
Educate executives	70%	
Create evangelism	75%	✓
LEVEL 2		
Identify metrics	40%	
Enforce gates	50%	✓
Publish data	30%	✓
LEVEL 3		
Maturity tracking application	40%	✓
Marketing & culture program	45%	

Maturity Levels

OWASP SAMM

Level 1
Quality Criteria



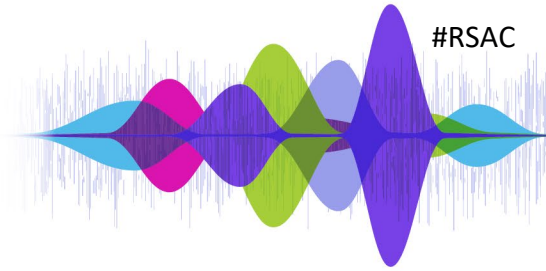
Activity Score:
0 - 1.0

STRATEGY & METRICS			
Create and promote			
Level	**Question & Criteria's**	**Answer**	**Rating**
1	Understand risk appetite for apps?		0,75
	✓ You capture risk appetite ✓ Risks are vetted and approved ✓ Risks are documented	No Yes, general risks Yes, org-specific risks ✓ Yes, also opportunities	
2	Strategic plan defined?		
	✓ Plan reflects business prior. ✓ Includes budget ✓ Lays out a roadmap	No, Yes, reviewed annually ✓ Yes, consulted on decisions Yes aligned with strategy	
3	AppSec strategic plan regularly reviewed?		
	✓ Based on strategic changes Risks are vetted and approved	✓ No Yes, but ad-hoc Yes, at regular times	

Primary Categories

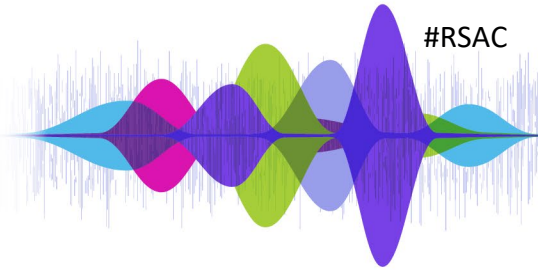
BSIMM	OWASP SAMM
4 high level domains: • Governance • Intelligence • SSDL Touchpoints • Deployment	5 business functions: • Governance • Design • Implementation • Verification • Operations

Secondary Categories



BSIMM (~120 activities)	OWASP SAMM (90 activities)
3 practices per domain	3 security practices per business function
Governance • Strategy & Metrics • Compliance & Policy • Training	Governance • Strategy & Metrics • Policy & Compliance • Education & Guidance
Intelligence • Attack Models • Security Features & Design • Standards & Requirements	Design • Threat Assessment • Security Requirements • Secure Architecture

Secondary Categories - Continued



BSIMM (~120 activities)

SSDL Touchpoints
- Architecture Analysis
- Code Review
- Security Testing

Deployment
- Penetration Testing
- Software Environment
- Config Mgmt / Vuln Mgmt

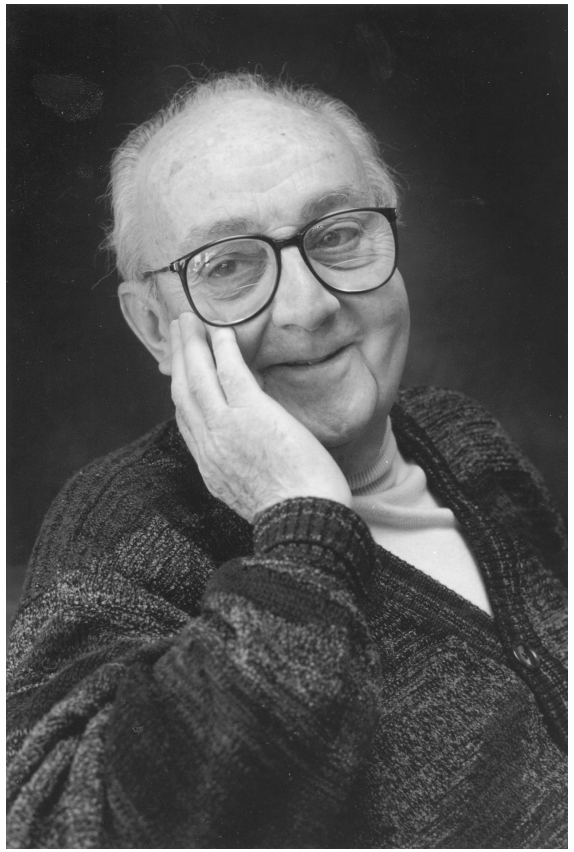
OWASP SAMM (90 activities)

Implementation
- Secure Build
- Secure Deployment
- Defect Management

Verification
- Architecture Analysis
- Requirements-driven Testing
- Security Testing

Operations
- Incident Management
- Environment Management
- Operational Management

Which Model is Better?



"All models are wrong, but some are useful"

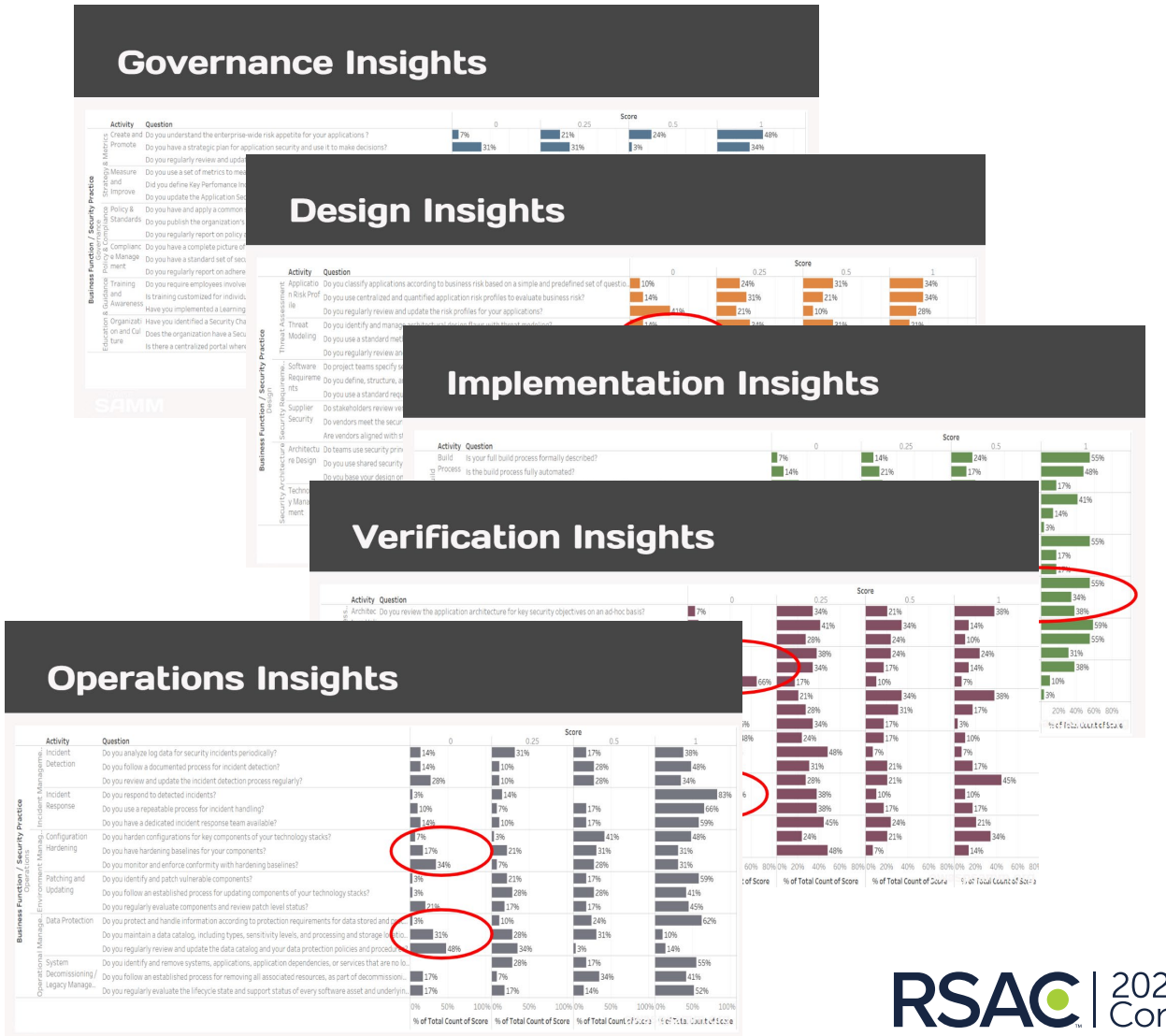
- George Box

Other Key Factors to Consider

Feature	BSIMM	SAMM
Purpose	Descriptive: Observes and reports what organizations do for software security.	Prescriptive: Offers guidance for implementing security activities.
Availability	Requires external assessment; detailed report sharing high level results is available publicly.	Open-source OWASP flagship project; supports self-assessment.
Tooling	Proprietary tools by a vendor.	Supported by various free tools like OpenSAMMY, SAMMWise, Toolbox in .xlsx, .gsheet format.
Benchmarking	3rd party assessment enables consistency between evaluation of different organizations.	Benchmarking is available based on anonymized data donated by members of the SAMM practitioner community.

Benchmarks

- BSIMM
  - Data based on consistent, recent assessment of ~130 organizations
- OWASP SAMM
  - Anonymized data donated by SAMM practitioners



Guidance for Improvement

OWASP SAMM

- Community driven content available per activity on the owaspsamm.org:
  - Activity benefit
  - Detailed description
  - Question for assessment
  - Quality criteria and answers
  - Guidance for implementation
- Channels for support: Meetup

BSIMM

- Comprehensive benchmarking report and expert guidance for improvement provided by the assessment vendor.
- Can be useful for justifying requests for additional investment.

Apply What You Have Learned Today

- Next week
  - Review your organization's current approach to software security.
  - Identify whether SAMM, BSIMM, or a combination of both best fits your needs.
  - Discuss with key stakeholders how security maturity is currently assessed and improved.
- In 3 months
  - Conduct a preliminary assessment using SAMM or BSIMM.
  - Define clear security maturity goals and priorities for your organization.
  - Start implementing small, actionable improvements based on the assessment findings.
- Remember
  - Every company using software should leverage a maturity model to assess, plan, and track progress in application security.
  - Application security is a continuous journey, not a one-time exam. Long-term trends and improvements matter far more than a single assessment at any given moment.

RSAC 2025 Conference

Many Voices.
One Community.

Helpful Resources

https://owaspsamm.org/
https://www.bsimm.com/

Caroline WONG
Director of Cybersecurity
Teradata
https://www.linkedin.com/in/carolinewmwong

Nariman AGA-TAGIYEV
Application Security Architect
Dassault Systemes SE
https://www.linkedin.com/in/aganariman/